Results for "((((bios or boot) and (symmetric key))<in>metadata)) <and> (pyr >= 1950 <and> p..." e-mail
Your search matched **0** documents.
A maximum of **100** results are displayed, **25** to a page, sorted by **Relevance** in **Descending** order.

» Search Options

View Session History

New Search

Modify Search

((((bios or boot) and (symmetric key))<in>metadata)) <and> (pyr >= 1950 <and> pyr Search

Check to search only within this results set

Display Format: Citation Citation & Abstract

» Key

IEEE JNL	IEEE Journal or Magazine
IET JNL	IET Journal or Magazine
IEEE CNF	IEEE Conference Proceeding
IET CNF	IET Conference Proceeding
IEEE STD	IEEE Standard

No results were found.

Please edit your search criteria and try again. Refer to the Help pages if you need assistan search.

Results for "((((basic input output system) or (bios code) and (symmetric key))<in>metadata)) <and> (..." e-mail
Your search matched 0 documents.
A maximum of 100 results are displayed, 25 to a page, sorted by Relevance in Descending order.

» Search Options

View Session History

New Search

Modify Search

((((basic input output system) or (bios code) and (symmetric key))<in>metadata)) <an Search

☐ Check to search only within this results set

Display Format: ◉ Citation ○ Citation & Abstract

» Key

IEEE JNL	IEEE Journal or Magazine
IET JNL	IET Journal or Magazine
IEEE CNF	IEEE Conference Proceeding
IET CNF	IET Conference Proceeding
IEEE STD	IEEE Standard

No results were found.

Please edit your search criteria and try again. Refer to the Help pages if you need assistan search.

Results for "(((run bios code) and access* and key<in>metadata)) <and> (pyr >= 1950 <and&g..." e-mail
Your search matched 0 documents.
A maximum of 100 results are displayed, 25 to a page, sorted by Relevance in Descending order.

» Search Options

View Session History

New Search

Modify Search

(((run bios code) and access* and key<in>metadata)) <and> (pyr >= 1950 <and> Search

Check to search only within this results set

Display Format: Citation Citation & Abstract

» Key

IEEE JNL	IEEE Journal or Magazine
IET JNL	IET Journal or Magazine
IEEE CNF	IEEE Conference Proceeding
IET CNF	IET Conference Proceeding
IEEE STD	IEEE Standard

No results were found.

Please edit your search criteria and try again. Refer to the Help pages if you need assistan search.

Results for "(bios code and key<in>metadata)"
Your search matched 0 documents.
A maximum of 100 results are displayed, 25 to a page, sorted by Relevance in Descending order.

e-mail

» Search Options

View Session History

New Search

Modify Search

(bios code and key<in>metadata) Search

☐ Check to search only within this results set

Display Format: ◉ Citation ○ Citation & Abstract

» Key

IEEE JNL	IEEE Journal or Magazine
IET JNL	IET Journal or Magazine
IEEE CNF	IEEE Conference Proceeding
IET CNF	IET Conference Proceeding
IEEE STD	IEEE Standard

No results were found.

Please edit your search criteria and try again. Refer to the Help pages if you need assistan search.

Indexed by Inspec®

Results for "((power on self test system) and key<in>metadata)" e-mail
Your search matched 0 documents.
A maximum of 100 results are displayed, 25 to a page, sorted by Relevance in Descending order.

» Search Options

View Session History

New Search

Modify Search

((power on self test system) and key<in>metadata) Search

☐ Check to search only within this results set

Display Format: ◉ Citation ○ Citation & Abstract

» Key

IEEE JNL	IEEE Journal or Magazine
IET JNL	IET Journal or Magazine
IEEE CNF	IEEE Conference Proceeding
IET CNF	IET Conference Proceeding
IEEE STD	IEEE Standard

No results were found.

Please edit your search criteria and try again. Refer to the Help pages if you need assistan search.

Results for "(((basic input output system) or bios) and stor* and key<in>metadata)" e-mail
Your search matched **27** of **1597822** documents.
A maximum of **100** results are displayed, **25** to a page, sorted by **Relevance** in **Descending** order.

» Search Options

View Session History

New Search

Modify Search

(((basic input output system) or bios) and stor* and key<in>metadata) Search

Check to search only within this results set

Display Format: Citation Citation & Abstract

» Key

IEEE JNL	IEEE Journal or Magazine
IET JNL	IET Journal or Magazine
IEEE CNF	IEEE Conference Proceeding
IET CNF	IET Conference Proceeding
IEEE STD	IEEE Standard

view selected items Select All Deselect All

1. **Enhancing PC Security with a U-Key**
Peng Shaunghe; Han Zhen;
Security & Privacy Magazine, IEEE
Volume 4, Issue 5, Sept.-Oct. 2006 Page(s):34 - 39
Digital Object Identifier 10.1109/MSP.2006.118
AbstractPlus | Full Text: PDF(2221 KB) IEEE JNL
Rights and Permissions

2. **Achieving deterministic, hard real-time control on an IBM-compatible PC: configuration guideline**
Zhang, J.; Lumia, R.; Wood, J.; Starr, G.;
Systems, Man and Cybernetics, 2005 IEEE International Conference on
Volume 1, 10-12 Oct. 2005 Page(s):293 - 299 Vol. 1
Digital Object Identifier 10.1109/ICSMC.2005.1571161
AbstractPlus | Full Text: PDF(216 KB) IEEE CNF
Rights and Permissions

3. **A trusted open platform**
England, P.; Lampson, B.; Manferdelli, J.; Willman, B.;
Computer
Volume 36, Issue 7, July 2003 Page(s):55 - 62
Digital Object Identifier 10.1109/MC.2003.1212691
AbstractPlus | References | Full Text: PDF(273 KB) IEEE JNL
Rights and Permissions

4. **Architecture for protecting critical secrets in microprocessors**
Lee, R.B.; Kwan, P.C.S.; McGregor, J.P.; Dwoskin, J.; Zhenghong Wang;
Computer Architecture, 2005. ISCA '05. Proceedings. 32nd International Symp
4-8 June 2005 Page(s):2 - 13
Digital Object Identifier 10.1109/ISCA.2005.14
AbstractPlus | Full Text: PDF(152 KB) IEEE CNF
Rights and Permissions

5. **Data general desktop generation model 10: Architecture and implementat**
Miller, R.C.; Wade, D.A.; Wallis, C.;
Proceedings of the IEEE
Volume 72, Issue 3, March 1984 Page(s):312 - 321

AbstractPlus | Full Text: PDF(932 KB) IEEE JNL
Rights and Permissions

6. **Persistent access control to prevent piracy of digital information**
Schneck, P.B.;
Proceedings of the IEEE
Volume 87, Issue 7, July 1999 Page(s):1239 - 1250
Digital Object Identifier 10.1109/5.771075
AbstractPlus | References | Full Text: PDF(744 KB) IEEE JNL
Rights and Permissions

7. **Adding Transparent Internetworking to a LAN Application Interface**
Janson, P.; Cockburn, A.;
Selected Areas in Communications, IEEE Journal on
Volume 5, Issue 9, Dec 1987 Page(s):1471 - 1479
AbstractPlus | Full Text: PDF(1096 KB) IEEE JNL
Rights and Permissions

8. **Ensemble-level Power Management for Dense Blade Servers**
Ranganathan, P.; Leech, P.; Irwin, D.; Chase, J.;
Computer Architecture, 2006. ISCA '06. 33rd International Symposium on
2006 Page(s):66 - 77
Digital Object Identifier 10.1109/ISCA.2006.20
AbstractPlus | Full Text: PDF(325 KB) IEEE CNF
Rights and Permissions

9. **Trust-enhanced alteration scenario for universal computer**
Jiangchun Ren; Kui Dai; Zhiying Wang;
Dependable Computing, 2005. Proceedings. 11th Pacific Rim International Syr
12-14 Dec. 2005 Page(s):6 pp.
Digital Object Identifier 10.1109/PRDC.2005.60
AbstractPlus | Full Text: PDF(184 KB) IEEE CNF
Rights and Permissions

10. **Detecting stealth software with Strider GhostBuster**
Wang, Y.-M.; Beck, D.; Vo, B.; Roussev, R.; Verbowski, C.;
Dependable Systems and Networks, 2005. DSN 2005. Proceedings. Internatic
on
28 June-1 July 2005 Page(s):368 - 377
Digital Object Identifier 10.1109/DSN.2005.39
AbstractPlus | Full Text: PDF(232 KB) IEEE CNF
Rights and Permissions

11. **The Transmeta Code Morphing/spl trade/ Software: using speculation, re adaptive retranslation to address real-life challenges**
Dehnert, J.C.; Grant, B.K.; Banning, J.P.; Johnson, R.; Kistler, T.; Klaiber, A.; I
Code Generation and Optimization, 2003. CGO 2003. International Symposiur
23-26 March 2003 Page(s):15 - 24
Digital Object Identifier 10.1109/CGO.2003.1191529
AbstractPlus | Full Text: PDF(391 KB) IEEE CNF
Rights and Permissions

12. **Embedded Pentium(R) processor system design for Windows CE**
Gallas, B.; Verma, V.;
WESCON/98
15-17 Sept. 1998 Page(s):114 - 123
Digital Object Identifier 10.1109/WESCON.1998.716432
AbstractPlus | Full Text: PDF(660 KB) IEEE CNF
Rights and Permissions

☐ **13. The future is in the PC cards**
Sternglass, D.;
Spectrum, IEEE
Volume 29, Issue 6, June 1992 Page(s):46 - 50
Digital Object Identifier 10.1109/6.254020
AbstractPlus | Full Text: PDF(588 KB) IEEE JNL
Rights and Permissions

☐ **14. The first decade of personal computers**
Gupta, A.; Toong, H.-M.D.;
Proceedings of the IEEE
Volume 72, Issue 3, March 1984 Page(s):246 - 258
AbstractPlus | Full Text: PDF(1332 KB) IEEE JNL
Rights and Permissions

☐ **15. Technology directions for portable computers**
Harris, E.P.; Depp, S.W.; Pence, W.E.; Kirkpatrick, S.; Sri-Jayantha, M.; Troutı
Proceedings of the IEEE
Volume 83, Issue 4, April 1995 Page(s):636 - 658
Digital Object Identifier 10.1109/5.371971
AbstractPlus | Full Text: PDF(2040 KB) IEEE JNL
Rights and Permissions

☐ **16. International development of Taiwan's information industry: an empirical human resource strategy of overseas subsidiaries**
Shang-Jyh Liu; Ti-Lun Huang; Quang-Hua Chen;
Engineering Management, IEEE Transactions on
Volume 45, Issue 3, Aug. 1998 Page(s):296 - 310
Digital Object Identifier 10.1109/17.704253
AbstractPlus | References | Full Text: PDF(240 KB) IEEE JNL
Rights and Permissions

☐ **17. The Resurrecting Duckling: security issues for ubiquitous computing**
Stajano, F.; Anderson, R.;
Computer
Volume 35, Issue 4, Part Supplement, April 2002 Page(s):22 - 26
Digital Object Identifier 10.1109/MC.2002.1012427
AbstractPlus | References | Full Text: PDF(530 KB) IEEE JNL
Rights and Permissions

☐ **18. Design of Smart Phone-Oriented Embedded Real-time Operating System**
Jigang Wang; Guochang Gu; Shibo Xie; Lifeng Xu;
Computer and Computational Sciences, 2006. IMSCCS '06. First International Symposiums on
Volume 2, 20-24 April 2006 Page(s):758 - 763
Digital Object Identifier 10.1109/IMSCCS.2006.210
AbstractPlus | Full Text: PDF(184 KB) IEEE CNF
Rights and Permissions

☐ **19. Minos: Control Data Attack Prevention Orthogonal to Memory Model**
Crandall, J.R.; Chong, F.T.;
Microarchitecture, 2004. MICRO-37 2004. 37th International Symposium on
04-08 Dec. 2004 Page(s):221 - 232
Digital Object Identifier 10.1109/MICRO.2004.26
AbstractPlus | Full Text: PDF(264 KB) IEEE CNF
Rights and Permissions

☐ **20. A study of heat generation and transport in tunnel junctions**
Yongho Sungtaek Ju;
Thermal and Thermomechanical Phenomena in Electronic Systems, 2004. ITH
Ninth Intersociety Conference on
Volume 2, 1-4 June 2004 Page(s):411 - 417 Vol.2
Digital Object Identifier 10.1109/ITHERM.2004.1318312
AbstractPlus | Full Text: PDF(521 KB) IEEE CNF
Rights and Permissions

☐ **21. Smart card for smart campus: KFUPM case study**
Halawani, T.; Mohandes, M.;
Electronics, Circuits and Systems, 2003. ICECS 2003. Proceedings of the 200
International Conference on
Volume 3, 14-17 Dec. 2003 Page(s):1252 - 1255 Vol.3
Digital Object Identifier 10.1109/ICECS.2003.1301741
AbstractPlus | Full Text: PDF(1461 KB) IEEE CNF
Rights and Permissions

☐ **22. Breakpoint debugging mechanism for microprocessor design**
Wang Danghui; Gao Deyuan; Li Tao;
ASIC, 2003. Proceedings. 5th International Conference on
Volume 1, 21-24 Oct. 2003 Page(s):456 - 458 Vol.1
Digital Object Identifier 10.1109/ICASIC.2003.1277584
AbstractPlus | Full Text: PDF(285 KB) IEEE CNF
Rights and Permissions

☐ **23. Electrowetting-based on-chip sample processing for integrated microflui**
Fair, R.B.; Srinivasan, V.; Ren, H.; Paik, P.; Pamula, V.K.; Pollack, M.G.;
Electron Devices Meeting, 2003. IEDM '03 Technical Digest. IEEE Internationa
8-10 Dec. 2003 Page(s):32.5.1 - 32.5.4
Digital Object Identifier 10.1109/IEDM.2003.1269396
AbstractPlus | Full Text: PDF(383 KB) IEEE CNF
Rights and Permissions

☐ **24. YES2 DHS: a space tether control subsystem**
Dueck, S.; Gadhok, N.; Kinsner, M.; Kraut, J.; Tessier, T.; Kinsner, W.;
Electrical and Computer Engineering, 2003. IEEE CCECE 2003. Canadian Co
Volume 2, 4-7 May 2003 Page(s):1287 - 1292 vol.2
Digital Object Identifier 10.1109/CCECE.2003.1226135
AbstractPlus | Full Text: PDF(683 KB) IEEE CNF
Rights and Permissions

☐ **25. Exploring the use of Hyper-Threading technology for multimedia applicat**
Intel/spl reg/ OpenMP compiler
Xinmin Tian; Yen-Kuang Chen; Girkar, M.; Ge, S.; Lienhart, R.; Shah, S.;
Parallel and Distributed Processing Symposium, 2003. Proceedings. Internatic
22-26 April 2003 Page(s):8 pp.
Digital Object Identifier 10.1109/IPDPS.2003.1213118
AbstractPlus | Full Text: PDF(325 KB) IEEE CNF
Rights and Permissions

Terms used: **bios** and **symmetric key** Found **12** of **205,978**

Sort results by: relevance
Display results: expanded form
Save results to a Binder
Search Tips
Open results in a new window
Try an Advanced Search
Try this search in The ACM Guide

Results 1 - 12 of 12

Relevance scale

1 Architecture for Protecting Critical Secrets in Microprocessors

Ruby B. Lee, Peter C. S. Kwan, John P. McGregor, Jeffrey Dwoskin, Zhenghong Wang
May 2005 **ACM SIGARCH Computer Architecture News , Proceedings of the 32nd annual international symposium on Computer Architecture ISCA '05**, Volume 33 Issue 2
Publisher: IEEE Computer Society, ACM Press
Full text available: pdf(143.62 KB) Additional Information: full citation, abstract, cited by, index terms

We propose "secret-protected (SP)" architecture to enable secure and convenient protection of critical secrets for a given user in an on-line environment. Keys are examples of critical secrets, and key protection and management is a fundamental problem ¿ often assumed but not solved ¿ underlying the use of cryptographic protection of sensitive files, messages, data and programs. SP-processors contain a minimalist set of architectural features that can be built into a general-purpose microprocess ...

2 Security as a new dimension in embedded system design: Security as a new dimension in embedded system design

Srivaths Ravi, Paul Kocher, Ruby Lee, Gary McGraw, Anand Raghunathan
June 2004 **Proceedings of the 41st annual conference on Design automation DAC '04**
Publisher: ACM Press
Full text available: pdf(209.10 KB) Additional Information: full citation, abstract, references, citings, index terms

The growing number of instances of breaches in information security in the last few years has created a compelling case for efforts towards secure electronic systems. Embedded systems, which will be ubiquitously used to capture, store, manipulate, and access data of a sensitive nature, pose several unique and interesting security challenges. Security has been the subject of intensive research in the areas of cryptography, computing, and networking. However, despite these efforts, *security is* ...

Keywords: *PDAs, architectures, battery life, cryptography, design, design methodologies, digital rights management, embedded systems, performance, security, security processing, security protocols, sensors, software attacks, tamper resistance, trusted computing, viruses*

3 Practical byzantine fault tolerance and proactive recovery

Miguel Castro, Barbara Liskov

November 2002 **ACM Transactions on Computer Systems (TOCS)**, Volume 20 Issue 4
Publisher: ACM Press

Full text available: pdf(1.63 MB) Additional Information: full citation, abstract, references, citings, index terms, review

Our growing reliance on online services accessible on the Internet demands highly available systems that provide correct service without interruptions. Software bugs, operator mistakes, and malicious attacks are a major cause of service interruptions and they can cause arbitrary behavior, that is, Byzantine faults. This article describes a new replication algorithm, BFT, that can be used to build highly available systems that tolerate Byzantine faults. BFT can be used in practice to implement re ...

Keywords: Byzantine fault tolerance, asynchronous systems, proactive recovery, state machine replication, state transfer

4 The Impact of Performance Asymmetry in Emerging Multicore Architectures

Saisanthosh Balakrishnan, Ravi Rajwar, Mike Upton, Konrad Lai
May 2005 **ACM SIGARCH Computer Architecture News , Proceedings of the 32nd annual international symposium on Computer Architecture ISCA '05**, Volume 33 Issue 2
Publisher: IEEE Computer Society, ACM Press
Full text available: pdf(287.94 KB) Additional Information: full citation, abstract, cited by, index terms

Performance asymmetry in multicore architectures arises when individual cores have different performance. Building such multicore processors is desirable because many simple cores together provide high parallel performance while a few complex cores ensure high serial performance. However, application developers typically assume computational cores provide equal performance, and performance asymmetry breaks this assumption. This paper is concerned with the behavior of commercial applications runn ...

5 Applications and compliance: Virtual monotonic counters and count-limited objects using a TPM without a trusted OS

Luis F. G. Sarmenta, Marten van Dijk, Charles W. O'Donnell, Jonathan Rhodes, Srinivas Devadas
November 2006 **Proceedings of the first ACM workshop on Scalable trusted computing STC '06**
Publisher: ACM Press
Full text available: pdf(447.59 KB) Additional Information: full citation, abstract, references, index terms

A trusted monotonic counter is a valuable primitive that enables a wide variety of highly scalable offline and decentralized applications that would otherwise be prone to replay attacks, including offline payment, e-wallets, virtual trusted storage, and digital rights management (DRM). In this paper, we show how one can implement a very large number of *virtual* monotonic counters on an untrusted machine with a Trusted Platform Module (TPM) or similar device, without relying on a trusted OS ...

Keywords: certified execution, e-wallet memory integrity checking, key delegation, stored-value, trusted storage

6 Efficient indexing data structures for flash-based sensor devices

Song Lin, Demetrios Zeinalipour-Yazti, Vana Kalogeraki, Dimitrios Gunopulos, Walid A. Najjar
November 2006 **ACM Transactions on Storage (TOS)**, Volume 2 Issue 4
Publisher: ACM Press
Full text available: pdf(1.45 MB) Additional Information: full citation, abstract, references, index terms

Flash memory is the most prevalent storage medium found on modern *wireless sensor devices (WSDs)*. In this article we present two external memory index structures for the efficient retrieval of records stored on the local flash memory of a WSD. Our index structures, *MicroHash* and *MicroGF (micro grid files)*, exploit the asymmetric read/write and wear characteristics of flash memory in order to offer high-performance indexing and searching capabilities in the presence of a low- ...

Keywords: Wireless sensor networks, access methods, flash memory

7 BASE: Using abstraction to improve fault tolerance

Miguel Castro, Rodrigo Rodrigues, Barbara Liskov
August 2003 **ACM Transactions on Computer Systems (TOCS)**, Volume 21 Issue 3
Publisher: ACM Press

Full text available: pdf(438.18 KB) Additional Information: full citation, abstract, references, citings, index terms

Software errors are a major cause of outages and they are increasingly exploited in malicious attacks. Byzantine fault tolerance allows replicated systems to mask some software errors but it is expensive to deploy. This paper describes a replication technique, BASE, which uses abstraction to reduce the cost of Byzantine fault tolerance and to improve its ability to mask software errors. BASE reduces cost because it enables reuse of off-the-shelf service implementations. It improves availability ...

Keywords: Byzantine fault tolerance, N-version programming, asynchronous systems, proactive recovery, state machine replication

8 An Integrated Framework for Dependable and Revivable Architectures Using Multicore Processors

Weidong Shi, Hsien-Hsin S. Lee, Laura `Falk, Mrinmoy Ghosh
May 2006 **ACM SIGARCH Computer Architecture News , Proceedings of the 33rd annual international symposium on Computer Architecture ISCA '06**, Volume 34 Issue 2
Publisher: IEEE Computer Society, ACM Press

Full text available: pdf(536.54 KB) Additional Information: full citation, abstract, index terms

This paper presents a high-availability system architecture called INDRA an INtegrated framework for Dependable and Revivable Architecture that enhances a multicore processor (or CMP) with novel security and fault recovery mechanisms. INDRA represents the first effort to create remote attack immune, self-healing network services using the emerging multicore processors. By exploring the property of a tightly-coupled multicore system, INDRA pioneers several concepts. It creates a hardware insulati ...

9 Pen computing: a technology overview and a vision

André Meyer
July 1995 **ACM SIGCHI Bulletin**, Volume 27 Issue 3
Publisher: ACM Press

Full text available: pdf(5.14 MB) Additional Information: full citation, abstract, citings, index terms

This work gives an overview of a new technology that is attracting growing interest in public as well as in the computer industry itself. The visible difference from other technologies is in the use of a pen or pencil as the primary means of interaction between a user and a machine, picking up the familiar pen and paper interface metaphor. From this follows a set of consequences that will be analyzed and put into context with other emerging technologies and visions.Starting with a short historic ...

10 Pioneer: verifying code integrity and enforcing untampered code execution on legacy systems

Arvind Seshadri, Mark Luk, Elaine Shi, Adrian Perrig, Leendert van Doorn, Pradeep Khosla
October 2005 **ACM SIGOPS Operating Systems Review , Proceedings of the twentieth ACM symposium on Operating systems principles SOSP '05**, Volume 39 Issue 5
Publisher: ACM Press

Full text available: pdf(264.30 KB) Additional Information: full citation, abstract, references, citings, index terms

We propose a primitive, called Pioneer, as a first step towards verifiable code execution on untrusted legacy hosts. Pioneer does not require any hardware support such as secure co-processors or CPU-architecture extensions. We implement Pioneer on an Intel Pentium IV Xeon processor. Pioneer can be used as a basic building block to build security systems. We demonstrate this by building a kernel rootkit detector.

Keywords: dynamic root of trust, rootkit detection, self-check-summing code, software-based code attestation, verifiable code execution

11 PC note

Eugene Styer
April 1997 **ACM SIGICE Bulletin**, Volume 22 Issue 4
Publisher: ACM Press
Full text available: pdf(741.61 KB) Additional Information: full citation, abstract, index terms

Now in segment nine we look at memory, video, and the PC bus. This is a bit more than I had planned, but with the changes coming up in SIGICE, I want to finish the remaining topics.

12 NetNews

Dennis Fowler
September 1999 **netWorker**, Volume 3 Issue 3
Publisher: ACM Press
Full text available: pdf(410.19 KB) html(27.87 KB) Additional Information: full citation, index terms

Results 1 - 12 of 12